Siri Artikel: Jadilah Pengguna Kewangan Dalam Talian Yang Bertanggungjawab
Bahagian 2

Selaras dengan perkembangan teknologi dalam perkhidmatan kewangan, risikonya juga turut berkembang. Baru-baru ini, terdapat peningkatan dalam penipuan malware melalui telefon pintar, mesej pancingan data (phishing), dan penipuan pembayaran dalam talian di rantau ini dan di Negara Brunei Darussalam. Untuk mengatasi ancaman siber ini dan melindungi pengguna-pengguna kewangan, institusi-institusi kewangan secara berterusan mengambil langkah-langkah untuk memperkukuhkan sistem perbankan masing-masing untuk mengelakkan pencerobohan data.

Pada masa yang sama, pengguna kewangan seperti awda juga memainkan peranan yang besar dalam menjaga keselamatan data peribadi serta memperkukuhkan peranti masing-masing. Dengan kerjasama institusi kewangan dan pengguna kewangan, kita boleh membina pertahanan yang kuat dan kukuh untuk menentang risiko kecurian maklumat dan kerugian kewangan, serta memastikan kita sentiasa selamat dalam talian.

Dalam siri artikel empat bahagian ini, kami akan mengongsikan beberapa tip dan nasihat untuk meningkatkan perlindungan daripada penipuan digital dengan menjadi pengguna kewangan di dalam talian yang bertanggungjawab. Pada minggu ini, kita akan membincangkan dengan lebih lanjut mengenai cara-cara untuk memperkukuhkan alat-alat peranti awda dan pentingnya kesedaran mengenai risiko-risiko dengan dunia digital seperti serangan siber, penipuan di atas talian dan juga kecurian maklumat peribadi.

1. Perkukuhkan alat peranti awda

Mempertingkatkan keselamatan semua alat peranti yang digunakan untuk membuat transaksi kewangan akan membantu melindungi data peribadi dan kewangan awda. Kebanyakan individu menjadi mangsa memuat turun malware dengan tidak sengaja setelah menekan pautan yang tidak diketahui asalnya. Ini boleh mengakibatkan maklumat perbankan dicuri atau akaun awda diakses tanpa kebenaran awda.

Perkara yang patut dilakukan

- Sentiasa mengemaskini sistem pengendalian, aplikasi, dan/atau firmware alat-alat peranti awda.
- Hanya memuat turun aplikasi melalui stor aplikasi yang rasmi seperti Apple AppStore atau Google PlayStore.
- Padam atau buang mana-mana aplikasi yang tidak diperlukan atau tidak digunakan lagi.
- Periksa semua aplikasi di dalam alat-alat peranti awda untuk memastikan tiada aplikasi yang mencurigakan.
- Tutup fungsi seperti rangkaian tanpa wayar, Bluetooth dan Komunikasi Medan Dekat ataupun Near Field Communication (NFC) bila tidak digunakan.

Perkara yang perlu dielakkan

- Elakkan daripada menekan pautan yang tidak diketahui atau tanpa pengesahan terlebih dahulu. Penipu biasanya menggunakan tajuk atau imej yang menarik perhatian mangsa untuk menekan pautan yang berkemungkinan mempunyai perisian malware.
- Pastikan telefon pintar awda tidak pernah dipecah sekat (jailbreaking) atau rooting.
- Elakkan daripada menyambungkan alat-alat peranti awda kepada port USB atau peranti yang tidak diketahui.

- Batalkan sebarang aktiviti yang mencurigakan terutamanya yang membuatkan alat peranti pintar awda mengeluarkan amaran.

2. Sentiasa berwaspada

Di era digital hari ini, kita perlu sentiasa berwaspada dan berjaga-jaga. Sama ada awda mengakses atau membincangkan maklumat awda di tempat awam, atau melayari internet dan membuat pembelian dalam talian, kita hendaklah peka terhadap sebarang risiko dan mengambil langkah-langkah untuk melindungi diri. Jika kita berwaspada dan proaktif, kita dapat mengurangkan risiko daripada menjadi mangsa serangan siber.

Perkara yang patut dilakukan

- Hanya berbincang mengenai urusan kewangan di tempat yang selamat dan tertutup bagi mengurangkan risiko dicuri dengar.
- Sentiasa berwaspada ketika membuat pembayaran di mana-mana kedai atau semasa menggunakan ATM di kawasan terpencil.
- Berhati-hati dengan persekitaran awda semasa memasukkan maklumat akaun dan daripada pandangan pengintip.
- Pastikan alamat laman web atau URL bank serta mana-mana platform membeli belah dalam talian bermula dengan 'https' atau mempunyai tanda ikon kunci.
- Periksa dan sahkan bahawa alamat laman web adalah betul, kerana penggodam boleh menggunakan huruf yang seakan sama dengan laman web asli untuk mengelirukan pengguna.

Perkara yang patut dielakkan

- Elakkan daripada membuat transaksi dalam talian melalui laman web yang mencurigakan atau tidak diketahui.
- Elakkan daripada membuat transaksi dalam talian melalui rangkaian tanpa wayar (Wi-Fi) awam, terutamanya Wi-Fi hotspot yang palsu.

Amalan-amalan mudah ini boleh membantu untuk memastikan maklumat dan transaksi kewangan awda selamat.

Nantikan artikel seterusnya untuk mendapatkan tip dan nasihat lanjut bagi melindungi diri awda dalam talian pada minggu depan!

Siri ini merupakan inisiatif bersama oleh:
Brunei Darussalam Central Bank (BDCB) (Instagram: @centralbank.brunei),
Pihak Berkuasa Industri Teknologi Info-komunikasi Negara Brunei Darussalam (AITI) (Instagram: @aiti.brunei),
Cyber Security Brunei (CSB) (Instagram: @csb.gov.bn), and
Brunei Association of Banks (BAB) (Laman web: www.bab.org.bn)